(e) The reviewer shall analyze the Hazard Log and/or any other hazard analysis documents for comprehensiveness and compliance with applicable railroad, vendor, supplier, industry, national, and international standards.

(f) The reviewer shall analyze all Fault Tree Analyses (FTA), Failure Mode and Effects Criticality Analysis (FMECA), and other hazard analyses for completeness, correctness, and compliance with applicable railroad, vendor, supplier, industry, national and international standards.

(g) The reviewer shall randomly select various safety-critical software, and hardware modules, if directed by FRA, for audit to verify whether the requirements of the applicable railroad, vendor, supplier, industry, national, and international standards were followed. The number of modules audited must be determined as a representative number sufficient to provide confidence that all unaudited modules were developed in compliance with the applicable railroad, vendor, supplier, industry, national, and international standards.

(h) The reviewer shall evaluate and comment on the plan for installation and test procedures of the product for revenue service.

(i) The reviewer shall prepare a final report of the assessment. The report shall be submitted to the railroad prior to the commencement of installation testing and contain at least the following information:

(1) Reviewer's evaluation of the adequacy of the PSP in the case of products developed under subpart H, or PTCSP for products developed under subpart I of this part, including the supplier's MTTHE and risk estimates for the product, and the supplier's confidence interval in these estimates;

(2) Product vulnerabilities, potentially hazardous failure modes, or potentially hazardous operating circumstances which the reviewer felt were not adequately identified, tracked, mitigated, and corrected by either the vendor or supplier or the railroad;

(3) A clear statement of position for all parties involved for each product vulnerability cited by the reviewer;

(4) Identification of any documentation or information sought by the reviewer that was denied, incomplete, or inadequate;

(5) A listing of each applicable vendor, supplier, industry, national, or international standard, procedure or process which was not properly followed;

(6) Identification of the software verification and validation procedures, as well as the hardware verification validation procedures if deemed appropriate by FRA, for the product's safety-critical applications, and the reviewer's evaluation of the adequacy of these procedures;

(7) Methods employed by the product manufacturer to develop safety-critical software;

(8) If deemed applicable by FRA, the methods employed by the product manufacturer to develop safety-critical hardware by generally acceptable techniques;

(9) Method by which the supplier or railroad addresses comprehensiveness of the product design which considers the safety elements listed in paragraph (b) of appendix C to this part.

[75 FR 2720, Jan. 15, 2010]

APPENDIX E TO PART 236—HUMAN-MACHINE INTERFACE (HMI) DESIGN

(a) This appendix provides human factors design criteria applicable to both subpart H and subpart I of this part. HMI design criteria will minimize negative safety effects by causing designers to consider human factors in the development of HMIs. The product design should sufficiently incorporate human factors engineering that is appropriate to the complexity of the product; the gender, educational, mental, and physical capabilities of the intended operators and maintainers; the degree of required human interaction with the component; and the environment in which the product will be used.

(b) As used in this section, ''designer'' means anyone who specifies requirements for—or designs a system or subsystem, or both, for—a product subject to subpart H or subpart I of this part, and ''operator'' means any human who is intended to receive information from, provide information to, or perform repairs or maintenance on a safety-critical product subject to subpart H or I of this part.

(c) Human factors issues the designers must consider with regard to the general function of a system include:

(1) *Reduced situational awareness and over-reliance.* HMI design must give an operator active functions to perform, feedback on the results of the operator's actions, and information on the automatic functions of the system as well as its performance. The operator must be ''in-the-loop.'' Designers must consider at a minimum the following methods of maintaining an active role for human operators:

(i) The system must require an operator to initiate action to operate the train and require an operator to remain ''in-the-loop'' for at least 30 minutes at a time;

(ii) The system must provide timely feedback to an operator regarding the system's automated actions, the reasons for such actions, and the effects of the operator's manual actions on the system;

(iii) The system must warn operators in advance when it requires an operator to take action;

(iv) HMI design must equalize an operator's workload; and

(v) HMI design must not distract from the operator's safety related duties.

(2) *Expectation of predictability and consistency in product behavior and communications.* HMI design must accommodate an operator's expectation of logical and consistent relationships between actions and results. Similar objects must behave consistently when an operator performs the same action upon them.

(3) *End user limited ability to process information.* HMI design must therefore minimize an operator's information processing load. To minimize information processing load, the designer must:

(i) Present integrated information that directly supports the variety and types of decisions that an operator makes;

(ii) Provide information in a format or representation that minimizes the time required to understand and act; and

(iii) Conduct utility tests of decision aids to establish clear benefits such as processing time saved or improved quality of decisions.

(4) *End user limited memory.* HMI design must therefore minimize an operator's information processing load.

(i) To minimize short-term memory load, the designer shall integrate data or information from multiple sources into a single format or representation (''chunking'') and design so that three or fewer ''chunks'' of information need to be remembered at any one time.

(ii) To minimize long-term memory load, the designer shall design to support recognition memory, design memory aids to minimize the amount of information that must be recalled from unaided memory when making critical decisions, and promote active processing of the information.

(d) Design systems that anticipate possible user errors and include capabilities to catch errors before they propagate through the system;

(1) Conduct cognitive task analyses prior to designing the system to better understand the information processing requirements of operators when making critical decisions; and

(2) Present information that accurately represents or predicts system states.

(e) When creating displays and controls, the designer must consider user ergonomics and shall:

(1) Locate displays as close as possible to the controls that affect them;

(2) Locate displays and controls based on an operator's position;

(3) Arrange controls to minimize the need for the operator to change position;

(4) Arrange controls according to their expected order of use;

(5) Group similar controls together;

(6) Design for high stimulus-response compatibility (geometric and conceptual);

(7) Design safety-critical controls to require more than one positive action to activate (e.g., auto stick shift requires two movements to go into reverse);

(8) Design controls to allow easy recovery from error; and

(9) Design display and controls to reflect specific gender and physical limitations of the intended operators.

(f) The designer shall also address information management. To that end, HMI design shall:

(1) Display information in a manner which emphasizes its relative importance;

(2) Comply with the ANSI/HFS 100–1988 standard;

(3) Utilize a display luminance that has a difference of at least 35cd/m2 between the foreground and background (the displays should be capable of a minimum contrast 3:1 with 7:1 preferred, and controls should be provided to adjust the brightness level and contrast level);

(4) Display only the information necessary to the user;

(5) Where text is needed, use short, simple sentences or phrases with wording that an operator will understand and appropriate to the educational and cognitive capabilities of the intended operator;

(6) Use complete words where possible; where abbreviations are necessary, choose a commonly accepted abbreviation or consistent method and select commonly used terms and words that the operator will understand;

(7) Adopt a consistent format for all display screens by placing each design element in a consistent and specified location;

(8) Display critical information in the center of the operator's field of view by placing items that need to be found quickly in the upper left hand corner and items which are not time-critical in the lower right hand corner of the field of view;

(9) Group items that belong together;

(10) Design all visual displays to meet human performance criteria under monochrome conditions and add color only if it will help the user in performing a task, and use color coding as a redundant coding technique;

(11) Limit the number of colors over a group of displays to no more than seven;

(12) Design warnings to match the level of risk or danger with the alerting nature of the signal; and

(13) With respect to information entry, avoid full QWERTY keyboards for data entry.

(g) With respect to problem management, the HMI designer shall ensure that the:

(1) HMI design must enhance an operator's situation awareness;

(2) HMI design must support response selection and scheduling; and

(3) HMI design must support contingency planning.

(h) Ensure that electronics equipment radio frequency emissions are compliant with appropriate Federal Communications Commission regulations. The FCC rules and regulations are codified in Title 47 of the Code of Federal Regulations (CFR).

(1) Electronics equipment must have appropriate FCC Equipment Authorizations. The following documentation is applicable to obtaining FCC Equipment Authorization:

(i) OET Bulletin Number 61 (October, 1992 Supersedes May, 1987 issue) FCC Equipment Authorization Program for Radio Frequency Devices. This document provides an overview of the equipment authorization program to control radio interference from radio transmitters and certain other electronic products and an overview of how to obtain an equipment authorization.

(ii) OET Bulletin 63: (October 1993) Understanding The FCC Part 15 Regulations for Low Power, Non-Licensed Transmitters. This document provides a basic understanding of the FCC regulations for low power, unlicensed transmitters, and includes answers to some commonly-asked questions. This edition of the bulletin does not contain information concerning personal communication services (PCS) transmitters operating under Part 15, Subpart D of the rules.

(iii) 47 Code of Federal Regulations Parts 0 to 19. The FCC rules and regulations governing PCS transmitters may be found in 47 CFR, Parts 0 to 19.

(iv) OET Bulletin 62 (December 1993) Understanding The FCC Regulations for Computers and other Digital Devices. This document has been prepared to provide a basic understanding of the FCC regulations for digital (computing) devices, and includes answers to some commonly-asked questions.

(2) Designers must comply with FCC requirements for Maximum Permissible Exposure limits for field strength and power density for the transmitters operating at frequencies of 300 kHz to 100 GHz and specific absorption rate (SAR) limits for devices operating within close proximity to the body. The Commission's requirements are detailed in parts 1 and 2 of the FCC's Rules and Regulations (47 CFR 1.1307(b), 1.1310, 2.1091, 2.1093). The following documentation is applicable to demonstrating whether proposed or existing transmitting facilities, operations or devices comply with limits for human exposure to radiofrequency RF fields adopted by the FCC:

(i) OET Bulletin No. 65 (Edition 97–01, August 1997), ''Evaluating Compliance With FCC Guidelines For Human Exposure To Radiofrequency Electromagnetic Fields'',

(ii) OET Bulletin No 65 Supplement A, (Edition 97–01, August 1997), OET Bulletin No 65 Supplement B (Edition 97–01, August 1997) and

(iii) OET Bulletin No 65 Supplement C (Edition 01–01, June 2001).

(3) The bulletin and supplements offer guidelines and suggestions for evaluating compliance. However, they are not intended to establish mandatory procedures. Other methods and procedures may be acceptable if based on sound engineering practice.

[75 FR 2720, Feb. 15, 2010]

APPENDIX F TO PART 236—MINIMUM REQUIREMENTS OF FRA DIRECTED INDEPENDENT THIRD-PARTY ASSESSMENT OF PTC SYSTEM SAFETY VERIFICATION AND VALIDATION

(a) This appendix provides minimum requirements for mandatory independent third-party assessment of PTC system safety verification and validation pursuant to subpart H or I of this part. The goal of this assessment is to provide an independent evaluation of the PTC system manufacturer's utilization of safety design practices during the PTC system's development and testing phases, as required by the applicable PSP, PTCDP, and PTCSP, the applicable requirements of subpart H or I of this part, and any other previously agreed-upon controlling documents or standards.

(b) The supplier may request advice and assistance of the independent third-party reviewer concerning the actions identified in paragraphs (c) through (g) of this appendix. However, the reviewer should not engage in design efforts in order to preserve the reviewer's independence and maintain the supplier's proprietary right to the PTC system.

(c) The supplier shall provide the reviewer access to any and all documentation that the reviewer requests and attendance at any design review or walkthrough that the reviewer determines as necessary to complete and accomplish the third party assessment. The reviewer may be accompanied by representatives of FRA as necessary, in FRA's judgment, for FRA to monitor the assessment.

(d) The reviewer shall evaluate with respect to safety and comment on the adequacy of the processes which the supplier applies to the design and development of the PTC system. At a minimum, the reviewer shall evaluate the supplier design and development process regarding the use of an appropriate design methodology. The reviewer may use the comparison processes and test procedures that have been previously agreed to with FRA. Based on these analyses, the reviewer shall identify and document any significant safety vulnerabilities which are not adequately mitigated by the supplier's (or user's) processes. Finally, the reviewer shall evaluate the adequacy of the railroad's applicable PSP or PTCSP, and any other